

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Nathan

Last Name: Jackson

Mailing Address: 1506 S. Rock Hill

City: Webster Groves

Country: United States

State or Province: MO

ZIP/Postal Code: 63119

Email Address: nathan@jackson-group.biz

Organization Name:

Comment: The implementation of this rule would raise security and legal concerns for many individuals and small businesses. I do not want to be put in a scenario where I have to choose between making a software decision that I feel increases the security, reliability, and functionality of my network vs. potentially exposing myself to legal action under FCC regulations.

Using free and open firmware that is available to the public for review assures that we do not encounter security issues due to unsecured services (or intentional backdoors) in our firmware. It can also be used to enable features that are not available in manufactures firmware. Firmware from Netgear, Linksys, Asus, and other companies has repeatedly been found to expose network resources.

Not being able to fully control and modify firmware on a device that I own is not acceptable. Having to wait for a manufacturer to release a patch to secure a service I can't disable is not acceptable. I buy devices that I need to fill a specific set of needs, and manufactures provide firmware that is tailored to the widest variety of possible uses. Not being able to easily remove or disable features in a manufacturers firmware puts networks at risk!

The implementation of this rule would raise security and legal concerns for many individuals and small businesses. I do not want to be put in a scenario where I have to choose between making a software decision that I feel increases the security, reliability, and functionality of my network vs. potentially exposing myself to legal action under FCC regulations.

Using free and open firmware that is available to the public for review assures that we do not encounter security issues due to unsecured services (or intentional backdoors) in our firmware. It can also be used to enable features that are not available in manufactures firmware. Firmware from Netgear, Linksys, Asus, and other companies has repeatedly been found to expose network resources.

Not being able to fully control and modify firmware on a device that I own is not acceptable. Having to wait for a manufacturer to release a patch to secure a service I can't disable is not acceptable. I buy devices that I need to fill a specific set of needs, and manufactures provide firmware that is tailored to the widest variety of possible uses. Not being able to easily remove or disable features in a manufacturers firmware puts networks at risk!

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: kyle

Last Name: ryans

Mailing Address: 3749 e taro lane

City: phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85050

Email Address: kyleryans32@gmail.com

Organization Name: independent

Comment: This submission is to ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

What you need to understand, is that current generation WiFi routers are more computer, and less router. WiFi routers include functionality to provide firewall protection, anti-virus protection, media server functionality, VPN functionality, web server functionality, etc.

The above mentioned services (which is far from conclusive) introduce the potential for zero-day exploits. Removing the public's ability to protect their own environment (forcing them to rely upon vendor's to fix their devices) is an example of the government slowly eroding individuals freedom.

Further, many times a consumer decides to purchase a router based on it's hardware, with the intent to install customized firmware to provide functionality they need. By preventing this ability, you are simply making it less economical for potential consumers to find hardware and customize it to their liking.

From a risk perspective, why would the FCC feel such freedom generates an unacceptable risk, considering a consumer can go buy a car that goes 180 MPH? The parallel is, a consumer can do more harm with a car that is designed to brake nearly every practical law for the general use of an automobile, than to take a router with the ability to modify it and break US law. Trusting a driver not to speed is acceptable, while trusting a user of a wireless device to not modify it for illegal use isn't?

This submission is to ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

What you need to understand, is that current generation WiFi routers are more computer, and less router. WiFi routers include functionality to provide firewall protection, anti-virus protection, media server functionality, VPN functionality, web server functionality, etc.

The above mentioned services (which is far from conclusive) introduce the potential for zero-day exploits. Removing the public's ability to protect their own environment (forcing them to rely upon vendor's to fix their devices) is an example of the government slowly eroding individuals freedom.

Further, many times a consumer decides to purchase a router based on it's hardware, with the intent to install customized

firmware to provide functionality they need. By preventing this ability, you are simply making it less economical for potential consumers to find hardware and customize it to their liking.

From a risk perspective, why would the FCC feel such freedom generates an unacceptable risk, considering a consumer can go buy a car that goes 180 MPH? The parallel is, a consumer can do more harm with a car that is designed to brake nearly every practical law for the general use of an automobile, than to take a router with the ability to modify it and break US law. Trusting a driver not to speed is acceptable, while trusting a user of a wireless device to not modify it for illegal use isn't?

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jason

Last Name: Howard

Mailing Address: 10224 Hile Street

City: Grass Valley

Country: United States

State or Province: CA

ZIP/Postal Code: 95945

Email Address:

Organization Name:

Comment: Hello-

I'm writing you today to voice my opinion that the FCC should make no rule that inhibits the public's ability to load their choice of firmware on their devices. Personally, this is very important to me, as I've run into several situations where the original device vendor's firmware is deficient or insecure in some way. Loading my own firmware on these devices was the only way to alleviate this issue.

Further, inhibiting the ability to load third party firmware will stifle innovation. Not everyone can build a wireless device. Many more, however, are able to write software. By locking down firmware, you essentially cut off the second group's ability to innovate.

Thank you for your time,  
Jason Howard, N6QED

Hello-

I'm writing you today to voice my opinion that the FCC should make no rule that inhibits the public's ability to load their choice of firmware on their devices. Personally, this is very important to me, as I've run into several situations where the original device vendor's firmware is deficient or insecure in some way. Loading my own firmware on these devices was the only way to alleviate this issue.

Further, inhibiting the ability to load third party firmware will stifle innovation. Not everyone can build a wireless device. Many more, however, are able to write software. By locking down firmware, you essentially cut off the second group's ability to innovate.

Thank you for your time,  
Jason Howard, N6QED

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: David

Last Name: Heinrich

Mailing Address: 5934 Kingfisher Lane

City: Clarkston

Country: United States

State or Province: MI

ZIP/Postal Code: 48346

Email Address: David.Heinrich@gmail.com

Organization Name:

Comment: No this is wrong. This is just like changing a carburetor on an engine. If I own a piece of equipment, I own it. Locking the firmware to the manufacture changes it to a lease that I am not in control of even if I paid for it. Look at what John Deer is trying to do with tractors. Are you in the employment of big companies or the US citizens? Please stop this NOW.

No this is wrong. This is just like changing a carburetor on an engine. If I own a piece of equipment, I own it. Locking the firmware to the manufacture changes it to a lease that I am not in control of even if I paid for it. Look at what John Deer is trying to do with tractors. Are you in the employment of big companies or the US citizens? Please stop this NOW.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Adam

Last Name: Hughes

Mailing Address: 670 Louis Henna Blvd. Apt 2209

City: Round Rock

Country: United States

State or Province: TX

ZIP/Postal Code: 78664

Email Address: null

Organization Name: null

Comment: I am fully against this proposed regulation as a detriment to innovation and freedom of the internet as a medium. Please vote against passing these regulations.

I am fully against this proposed regulation as a detriment to innovation and freedom of the internet as a medium. Please vote against passing these regulations.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: William

Last Name: Overstreet

Mailing Address: 8711 Coral Dawn Ct

City: Temple Terrace

Country: United States

State or Province: FL

ZIP/Postal Code: 33637

Email Address:

Organization Name:

Comment: Depending on a hardware vendor to keep their shit together and supply security patches and software enhancements on existing platforms is quite possibly one of the worst ideas ever. A lot of the time, their promoted fix is to buy a new version of the device, instead of doing something silly like updating some software. Their track record for actually fixing something is usually not to do anything unless there is a massive public out-cry.

This sounds like an attempt to prevent people from modifying anything of a device they own, as long as, in this case, a 5GHz radio is installed. This would effectively stop already permitted activities like replacing the vendor rom on a cellphone. I do wonder what plans there are for going after SDRs broadcasting in the 5GHz range.

Hurray for vendor lock-in with planned obsolescence.

Depending on a hardware vendor to keep their shit together and supply security patches and software enhancements on existing platforms is quite possibly one of the worst ideas ever. A lot of the time, their promoted fix is to buy a new version of the device, instead of doing something silly like updating some software. Their track record for actually fixing something is usually not to do anything unless there is a massive public out-cry.

This sounds like an attempt to prevent people from modifying anything of a device they own, as long as, in this case, a 5GHz radio is installed. This would effectively stop already permitted activities like replacing the vendor rom on a cellphone. I do wonder what plans there are for going after SDRs broadcasting in the 5GHz range.

Hurray for vendor lock-in with planned obsolescence.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Bryan

Last Name: Prather-Huff

Mailing Address: 111 S Governor St.

City: Iowa City

Country: United States

State or Province: IA

ZIP/Postal Code: 52240

Email Address: bryan@pratherhuff.com

Organization Name: bryan@pratherhuff.com

Comment: While the spirit of this regulation may be protecting consumers and consumer products from damaging effects caused by misuse and misconfiguration, the realistic result of this legislation is a broad stroke of dangerous restriction on the ability for professionals and learned consumers to use their devices effectively. As a consumer and IT professional I find it disheartening that products which I rely on, on a near daily basis, such as Linux based router firmwares (Tomato, DDWRT), may suddenly be rendered illegal and impossible to use on new consumer devices. Regulations like this extend a large air of disrespect to well matured projects, especially Open Source, and are threatening to developers. In summary, DON'T PASS NEEDLESSLY BROAD LANGUAGED REGULATIONS.

While the spirit of this regulation may be protecting consumers and consumer products from damaging effects caused by misuse and misconfiguration, the realistic result of this legislation is a broad stroke of dangerous restriction on the ability for professionals and learned consumers to use their devices effectively. As a consumer and IT professional I find it disheartening that products which I rely on, on a near daily basis, such as Linux based router firmwares (Tomato, DDWRT), may suddenly be rendered illegal and impossible to use on new consumer devices. Regulations like this extend a large air of disrespect to well matured projects, especially Open Source, and are threatening to developers. In summary, DON'T PASS NEEDLESSLY BROAD LANGUAGED REGULATIONS.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Wing

Last Name: S

Mailing Address: PO Box 141

City: Pinehurst

Country: United States

State or Province: MA

ZIP/Postal Code: 01866

Email Address:

Organization Name:

Comment: Hello,

I am writing today to express my opposition to the proposal for "Equipment Authorization and Electronic Labeling for Wireless Devices." As I understand it these new rules would lock down WiFi devices so that their firmware could not be updated by the consumer as they wish.

While I understand that user-customizable firmware can be used in ways that are not legal and harmful to other devices, most users who use customizable firmware do not intend to use the firmware in this manner.

Instead, user-customizable firmware is an invaluable tool for consumers. It can be used for businesses to provide customers restricted WiFi access so that only paying customers use it. It can be used to create custom networks for research. And, perhaps most importantly, to ensure for a more secure Internet, often times user-customizable firmware can be used to patch security flaws in existing WiFi equipment. I have seen many routers whose manufacturers do not update their firmware, leaving them vulnerable to security flaws discovered after the router was released. Because user-customizable firmware is often quickly updated by the community, patches for routers are often released by the community first.

Hello,

I am writing today to express my opposition to the proposal for "Equipment Authorization and Electronic Labeling for Wireless Devices." As I understand it these new rules would lock down WiFi devices so that their firmware could not be updated by the consumer as they wish.

While I understand that user-customizable firmware can be used in ways that are not legal and harmful to other devices, most users who use customizable firmware do not intend to use the firmware in this manner.

Instead, user-customizable firmware is an invaluable tool for consumers. It can be used for businesses to provide customers restricted WiFi access so that only paying customers use it. It can be used to create custom networks for research. And, perhaps most importantly, to ensure for a more secure Internet, often times user-customizable firmware can be used to patch security flaws in existing WiFi equipment. I have seen many routers whose manufacturers do not update their firmware, leaving them vulnerable to security flaws discovered after the router was released. Because user-customizable firmware is often quickly updated by the community, patches for routers are often released by the community first.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jonathan

Last Name: Mayo

Mailing Address: 3356 Holly Dr

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95127

Email Address: jon@rm-f.net

Organization Name:

Comment: A requirement that prevents operators of a WiFi device from modifying, enhancing or repairing the software of a device provided by the original manufacturer is a troubling proposal.

Often we have to update firmware on devices that are no longer properly supported by the manufacturer to stay compliant with internet standards and remain good netizens. The problem of radio interference is not the only problem a device faces, as the internet protocols and websites themselves can suffer denial-of-service or unreliable behavior due to software defects. Many open source communities have form to repair software defects and add enhancements on the network layer to keep devices operating.

A requirement that prevents operators of a WiFi device from modifying, enhancing or repairing the software of a device provided by the original manufacturer is a troubling proposal.

Often we have to update firmware on devices that are no longer properly supported by the manufacturer to stay compliant with internet standards and remain good netizens. The problem of radio interference is not the only problem a device faces, as the internet protocols and websites themselves can suffer denial-of-service or unreliable behavior due to software defects. Many open source communities have form to repair software defects and add enhancements on the network layer to keep devices operating.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: RobRoy

Last Name: kelly

Mailing Address: 212 N Sturgis

City: munkato

Country: United States

State or Province: MN

ZIP/Postal Code: 56001

Email Address:

Organization Name:

Comment: most commercial wifi routers have serious and numerous bugs most of which are not fixed or corrected in a timely manner. the open source router programs written to be installed on some of the more common wifi routers are the only way to maintain a secure and up to date system. why would you want to disable one of the better and cheaper ways to maintain internet security?

most commercial wifi routers have serious and numerous bugs most of which are not fixed or corrected in a timely manner. the open source router programs written to be installed on some of the more common wifi routers are the only way to maintain a secure and up to date system. why would you want to disable one of the better and cheaper ways to maintain internet security?

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Karl

Last Name: Kurbjun

Mailing Address: 1304 Patton St.

City: Fort Collins

Country: United States

State or Province: CO

ZIP/Postal Code: 80524

Email Address: kkurbjun@gmail.com

Organization Name:

Comment: I understand the desire to prevent modification of the radio firmware, but anything beyond that is needlessly overstepping the FCC's charter.

This should not be used to prevent installing firmware such as DD-WRT as suggested by the SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES document: [https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking\\_number=39498](https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking_number=39498)

Having the ability to install DD-WRT in many cases results in a more secure router particularly with older routers that are not receiving firmware updates from the manufacturer but end up with published security vulnerabilities.

Again, I understand the purpose of locking down the SDR firmware, but that should not take priority over user's rights to devices they own.

I understand the desire to prevent modification of the radio firmware, but anything beyond that is needlessly overstepping the FCC's charter.

This should not be used to prevent installing firmware such as DD-WRT as suggested by the SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES document: [https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking\\_number=39498](https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking_number=39498)

Having the ability to install DD-WRT in many cases results in a more secure router particularly with older routers that are not receiving firmware updates from the manufacturer but end up with published security vulnerabilities.

Again, I understand the purpose of locking down the SDR firmware, but that should not take priority over user's rights to devices they own.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jon

Last Name: Tyler

Mailing Address: PO Box 757

City: Ocala

Country: United States

State or Province: FL

ZIP/Postal Code: 34478

Email Address:

Organization Name:

Comment: Government should not be in the business of removing the rights consumers to modify legally purchased products in any way we choose, so long as it does not violate the rights of others.

If I choose to repair a device that the manufacturer does not provide a fix for, that is my right. If you remove that right, you are forcing Americans to purchase a replacement product.

Government should not be in the business of removing the rights consumers to modify legally purchased products in any way we choose, so long as it does not violate the rights of others.

If I choose to repair a device that the manufacturer does not provide a fix for, that is my right. If you remove that right, you are forcing Americans to purchase a replacement product.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Stephen

Last Name: Deal

Mailing Address: 44 Rolling Hill Drive

City: Fairport

Country: United States

State or Province: NY

ZIP/Postal Code: 14450-9375

Email Address: devodl@gmail.com

Organization Name:

Comment: FCC please explain the existing problem you are trying to fix with the imposition of these rules. How extensive is the alleged problem that warrants such action?

In other words the FCC must JUSTIFY with accurate metrics the need for additional government regulation.

Americans demand the Freedom to choose and modify the firmware on their devices.

This Freedom does not imply that people will automatically violate FCC regulations. If the FCC chooses to impose these draconian measures then market forces will simply expand the availability of open source hardware and devices.

The proposed FCC rules that take away the ability of users to install the software of their choosing on their computing devices.

- Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

FCC please explain the existing problem you are trying to fix with the imposition of these rules. How extensive is the alleged problem that warrants such action?

In other words the FCC must JUSTIFY with accurate metrics the need for additional government regulation.

Americans demand the Freedom to choose and modify the firmware on their devices.

This Freedom does not imply that people will automatically violate FCC regulations. If the FCC chooses to impose these draconian measures then market forces will simply expand the availability of open source hardware and devices.

The proposed FCC rules that take away the ability of users to install the software of their choosing on their computing devices.

- Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and

companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Andrew

Last Name: Bradford

Mailing Address: 1870 Halesworth Ln

City: Ontario

Country: United States

State or Province: NY

ZIP/Postal Code: 14519

Email Address: bradfa@gmail.com

Organization Name:

Comment: Please do not restrict my ability to install software of my choosing on the computing devices which I have purchased.

I have owned 3 different wifi routers over the past decade. In all 3 cases, after about 1 year from when I purchased each router, the manufacturers all would decide to stop providing software updates for the routers. This left me with having a choice to do one of 3 things:

1. Buy another router.
2. Continue to use my router without any updates, exposing my router to known and published security vulnerabilities.
3. Install software on my router which was not provided by the router manufacturer.

For one of my routers, I decided to buy a different router. For another, I installed an open-source software distribution of Linux which was not provided by my router manufacturer which solved many of the outstanding security issues with that router and provided me with many years of service and software updates. In the 3rd case (my current wifi router), I have been running software on it which hasn't been updated by the manufacturer in 4 years and has known security vulnerabilities.

I'm currently shopping for a new router and I will not purchase one which does not have good support from a 3rd party open-source software distribution of Linux. This has proven to be the only way to keep my router software anywhere near up to date as the manufacturers do not continue to support products shortly after their launch.

The proposed new FCC rules will restrict my ability to have a secure network as I will not be able to install the software of my choosing and I will be stuck only using vendor provided software, which has been shown in 3 out of 3 of my last 10 years of wifi router ownership to be a very big letdown.

Please do not restrict my ability to install software of my choosing on the computing devices which I have purchased.

I have owned 3 different wifi routers over the past decade. In all 3 cases, after about 1 year from when I purchased each router, the manufacturers all would decide to stop providing software updates for the routers. This left me with having a choice to do one of 3 things:

1. Buy another router.
2. Continue to use my router without any updates, exposing my router to known and published security vulnerabilities.
3. Install software on my router which was not provided by the router manufacturer.

For one of my routers, I decided to buy a different router. For another, I installed an open-source software distribution of Linux which was not provided by my router manufacturer which solved many of the outstanding security issues with that router and provided me with many years of service and software updates. In the 3rd case (my current wifi router), I have been running software on it which hasn't been updated by the manufacturer in 4 years and has known security vulnerabilities.

I'm currently shopping for a new router and I will not purchase one which does not have good support from a 3rd party open-source software distribution of Linux. This has proven to be the only way to keep my router software anywhere near up to date as the manufacturers do not continue to support products shortly after their launch.

The proposed new FCC rules will restrict my ability to have a secure network as I will not be able to install the software of my choosing and I will be stuck only using vendor provided software, which has been shown in 3 out of 3 of my last 10 years of wifi router ownership to be a very big letdown.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Anthony

Last Name: Karakashian

Mailing Address: 124 Hartsdale Road

City: Rochester

Country: United States

State or Province: NY

ZIP/Postal Code: 14622

Email Address: savewifi@monstertruck.cc

Organization Name: NA

Comment: It's my understanding this proposed rule change would hinder my ability to flash devices I own with new versions of software that provide features the stock does not. This is not acceptable in any way.

First, as a user of Android-based products, I rely on the rich community of developers who produce custom versions of Android, so I can find the feature-set that more closely fits my needs. I buy a specific phone for the hardware specs, not the software it runs. If the software doesn't fit my needs, I can replace it, as it should be. You buy hardware for hardware, not the software that runs on it.

Second, as a person with a wifi network at home, I rely on the community to provide versions of the software for my router that provides a wider range of features. As a "computer" (for that is what it really is) that runs 24/7 in my house regardless of if it's being actively used, and is woefully underutilized for the majority of that time, I prefer it perform additional functions for me beyond simply routing packets to justify the electricity use in our current period of climate change.

I understand, the purpose of this rule is to ensure a piece of hardware equipped with a radio will never violate the levels it was shipped with; levels that were confirmed by the manufacturer to you as being acceptable to minimize interference with other products.

That's a reasonable requirement to make, however this rule is far over-compassing and would cause more damage in other areas and fields. Limit the rule to just modifying signal strength, as that's all you really want to do. Manufacturers can produce products that can't be modified through software, so make them do that and that alone. There. Easily fixed, and everyone's happy.

It's my understanding this proposed rule change would hinder my ability to flash devices I own with new versions of software that provide features the stock does not. This is not acceptable in any way.

First, as a user of Android-based products, I rely on the rich community of developers who produce custom versions of Android, so I can find the feature-set that more closely fits my needs. I buy a specific phone for the hardware specs, not the software it runs. If the software doesn't fit my needs, I can replace it, as it should be. You buy hardware for hardware, not the software that runs on it.

Second, as a person with a wifi network at home, I rely on the community to provide versions of the software for my router that provides a wider range of features. As a "computer" (for that is what it really is) that runs 24/7 in my house regardless of if it's being actively used, and is woefully underutilized for the majority of that time, I prefer it perform

additional functions for me beyond simply routing packets to justify the electricity use in our current period of climate change.

I understand, the purpose of this rule is to ensure a piece of hardware equipped with a radio will never violate the levels it was shipped with; levels that were confirmed by the manufacturer to you as being acceptable to minimize interference with other products.

That's a reasonable requirement to make, however this rule is far over-compassing and would cause more damage in other areas and fields. Limit the rule to just modifying signal strength, as that's all you really want to do. Manufacturers can produce products that can't be modified through software, so make them do that and that alone. There. Easily fixed, and everyone's happy.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Kelly

Last Name: Price

Mailing Address: 536 Greentree Terrace

City: Auburn

Country: United States

State or Province: AL

ZIP/Postal Code: 36832-2920

Email Address:

Organization Name:

Comment: Section 20 would prevent users from being able to fix software vulnerabilities in routers (a common occurrence). It would also stifle research into new wireless protocols. It is not acceptable.

Section 20 would prevent users from being able to fix software vulnerabilities in routers (a common occurrence). It would also stifle research into new wireless protocols. It is not acceptable.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Tyler

Last Name: McClure

Mailing Address: 228 Hunter Rd

City: Hayesville

Country: United States

State or Province: NC

ZIP/Postal Code: 28904

Email Address: t\_mcclure1@aol.com

Organization Name:

Comment: I completely disagree with your motion to control and in essence prohibit the "flashing" of firmware for routers and similar devices. You will only hold back innovation that allows us to advance in an ever changing world of technologies.

I completely disagree with your motion to control and in essence prohibit the "flashing" of firmware for routers and similar devices. You will only hold back innovation that allows us to advance in an ever changing world of technologies.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: cheryl

Last Name: miller

Mailing Address: 2704 Mintlaw ave

City: Henderson

Country: United States

State or Province: NV

ZIP/Postal Code: 89044

Email Address: cheraflu@yahoo.com

Organization Name:

Comment: the rule is way too general and applies to too many things that need to be modified by the owners of devices like routers. If you make it specific to modifications "proven to be designed to circumvent the law" or something it might not be so bad, but you should not be telling people they can't make any modifications.

the rule is way too general and applies to too many things that need to be modified by the owners of devices like routers.

If you make it specific to modifications "proven to be designed to circumvent the law" or something it might not be so bad, but you should not be telling people they can't make any modifications.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Derick

Last Name: Geisendorfer

Mailing Address: 2246 Meadowood Drive

City: Kronenwetter

Country: United States

State or Province: WI

ZIP/Postal Code: 54455

Email Address: dorfer21@hotmail.com

Organization Name:

Comment: This proposed regulation is bad and you should feel bad.

The decision to update/change the firmware on a router should remain with the consumer. To make it illegal to update firmware will open holes in unpatched routers as anytime a bug is found it would be up to the device manufacturer to release a patch. On devices as young as a year or two the manufacturer may not release a patch for the issue therefore keeping a known bug 'in the wild'.

They may not update the firmware on older routers anyway, but the user has then option to upload an Open Source firmware that doesn't have that vulnerability.

My one question, how many complaints have you received as a result of the option to install a custom firmware to a router and from whom?

This proposed regulation is bad and you should feel bad.

The decision to update/change the firmware on a router should remain with the consumer. To make it illegal to update firmware will open holes in unpatched routers as anytime a bug is found it would be up to the device manufacturer to release a patch. On devices as young as a year or two the manufacturer may not release a patch for the issue therefore keeping a known bug 'in the wild'.

They may not update the firmware on older routers anyway, but the user has then option to upload an Open Source firmware that doesn't have that vulnerability.

My one question, how many complaints have you received as a result of the option to install a custom firmware to a router and from whom?



# Common Sense

---

So rare it's a god damn super power.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Daniel

Last Name: Gary

Mailing Address: 1610 Cornfield Circle

City: Farmington

Country: United States

State or Province: NY

ZIP/Postal Code: 14425-9318

Email Address: flake@frontiernet.net

Organization Name: NA

Comment: I think making it so that open source software is effectively impossible to get certified is wrong. Many times the open source software is more responsive than manufacturers and blocking them from the hardware that I prefer to use is nonsense. Manufacturers in many cases stop releasing fixes to their firmware because they have newer products and don't want to be bothered spending money on something that they aren't making money on any longer. Free and open source software tends to give older equipment a longer lifespan because many of the people working on it don't care about the fact that the product isn't making money they care about it working properly. Plus shutting off this avenue to keeping older hardware and in some cases newer hardware relevant means that the hardware will just be thrown away instead of being used until it has died the permanent death so it goes to fill trash heaps much sooner than it would otherwise. Even if recycled, not all parts are recycled so this will add to the waste that our society is already generating making the world a worse place instead of a better place.

I think making it so that open source software is effectively impossible to get certified is wrong. Many times the open source software is more responsive than manufacturers and blocking them from the hardware that I prefer to use is nonsense. Manufacturers in many cases stop releasing fixes to their firmware because they have newer products and don't want to be bothered spending money on something that they aren't making money on any longer. Free and open source software tends to give older equipment a longer lifespan because many of the people working on it don't care about the fact that the product isn't making money they care about it working properly. Plus shutting off this avenue to keeping older hardware and in some cases newer hardware relevant means that the hardware will just be thrown away instead of being used until it has died the permanent death so it goes to fill trash heaps much sooner than it would otherwise. Even if recycled, not all parts are recycled so this will add to the waste that our society is already generating making the world a worse place instead of a better place.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: David

Last Name: Marsh

Mailing Address: 39317 Fallbrook Circle

City: Palmdale

Country: United States

State or Province: CA

ZIP/Postal Code: 93551

Email Address:

Organization Name:

Comment: Please reconsider the portion of these proposed rules that will effectively ban third-party firmware development and installation on wireless networking devices.

If the rule goes into effect as-is, it will make illegal a common practice of changing device firmware to add features and increase security. The security issues in particular are troubling, as many manufacturers fail to support their equipment with security updates after new models are on the market, typically on a 6-12 month cycle.

I personally have fixed security flaws in several consumer-grade WiFi routers after the manufacturers failed to support them. If the rule were in effect at the time, I would have had no choice but to discard these otherwise good devices.

There are many other reasons to change device firmware that do not cause the affected device to operate the radio elements in ways the violate the proposed or existing rules. In the case of consumer-grade WiFi routers, it is possible to add networking features that make them far more functional, but leave radio operation untouched. The proposed rule will, perhaps unintentionally, effectively destroy the ability to do this. Please reconsider.

Please reconsider the portion of these proposed rules that will effectively ban third-party firmware development and installation on wireless networking devices.

If the rule goes into effect as-is, it will make illegal a common practice of changing device firmware to add features and increase security. The security issues in particular are troubling, as many manufacturers fail to support their equipment with security updates after new models are on the market, typically on a 6-12 month cycle.

I personally have fixed security flaws in several consumer-grade WiFi routers after the manufacturers failed to support them. If the rule were in effect at the time, I would have had no choice but to discard these otherwise good devices.

There are many other reasons to change device firmware that do not cause the affected device to operate the radio elements in ways the violate the proposed or existing rules. In the case of consumer-grade WiFi routers, it is possible to add networking features that make them far more functional, but leave radio operation untouched. The proposed rule will, perhaps unintentionally, effectively destroy the ability to do this. Please reconsider.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: John

Last Name: Chamberlain

Mailing Address: PO Box 747

City: Natick

Country: United States

State or Province: MA

ZIP/Postal Code: 01760

Email Address: null

Organization Name: null

Comment: Concerning the aspect of the proposed rule "Equipment Authorization and Electronic Labeling for Wireless Devices" that would make it illegal for third parties to modify router ("certified equipment") firmware, I am submitting this comment opposing the proposed rule.

(First of all I find it obnoxious that your comment web site requires both Javascript (a security risk) and cookies (a privacy violation). I suggest you program your web site to use IP address rather than cookies and not use Javascript in the future.)

Secondly, let me just say for the record that I am opposed to non-elected persons and organizations making laws and I consider it unconstitutional and undemocratic for non-legislative bodies to be generating new legal statutes. I do not believe it is either proper nor the right of Congress to delegate to you or anyone else their law-making authority and it is wrong for you to be making federal laws without a vote in Congress.

Concerning the so-called "rule" itself:

Making it illegal for people to modify their own radio transmission equipment, including wireless routers, is an arrogant, oppressive and un-American idea which harkens back to the worst excesses of totalitarian regimes such as those of the Soviet Union and the so-called Deutsche Demokratische Republik who had many such "regulations" in their toolkit of oppression.

Choking off millions of people from using radio equipment in the ways they see fit, in a supposed effort to prevent radio interference, would be highly damaging to both the economy and technological progress. I say "supposed effort" because this rule will do nothing to hinder those small numbers people who for whatever reason are generating interference. This rule will only succeed in crushing the aspirations of millions of legitimate router users, while doing nothing to affect the tiny handful of interferers who will simply ignore your regulation. There are already "rules" in place concerning the generation of radio interference. Criminalizing modification of radio equipment adds nothing to these existing rules and will do nothing additional to prevent interference.

Concerning the aspect of the proposed rule "Equipment Authorization and Electronic Labeling for Wireless Devices" that would make it illegal for third parties to modify router ("certified equipment") firmware, I am submitting this comment opposing the proposed rule.

(First of all I find it obnoxious that your comment web site requires both Javascript (a security risk) and cookies (a privacy violation). I suggest you program your web site to use IP address rather than cookies and not use Javascript in

the future.)

Secondly, let me just say for the record that I am opposed to non-elected persons and organizations making laws and I consider it unconstitutional and undemocratic for non-legislative bodies to be generating new legal statutes. I do not believe it is either proper nor the right of Congress to delegate to you or anyone else their law-making authority and it is wrong for you to be making federal laws without a vote in Congress.

Concerning the so-called "rule" itself:

Making it illegal for people to modify their own radio transmission equipment, including wireless routers, is an arrogant, oppressive and un-American idea which harkens back to the worst excesses of totalitarian regimes such as those of the Soviet Union and the so-called Deutsche Demokratische Republik who had many such "regulations" in their toolkit of oppression.

Choking off millions of people from using radio equipment in the ways they see fit, in a supposed effort to prevent radio interference, would be highly damaging to both the economy and technological progress. I say "supposed effort" because this rule will do nothing to hinder those small numbers people who for whatever reason are generating interference. This rule will only succeed in crushing the aspirations of millions of legitimate router users, while doing nothing to affect the tiny handful of interferers who will simply ignore your regulation. There are already "rules" in place concerning the generation of radio interference. Criminalizing modification of radio equipment adds nothing to these existing rules and will do nothing additional to prevent interference.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Mark

Last Name: Craig

Mailing Address: 60 Creeks Edge Way

City: Sacramento

Country: United States

State or Province: CA

ZIP/Postal Code: 95823

Email Address: null

Organization Name: null

Comment: Isn't this delicious irony? The FCC's own "SamKnows" broadband survey project uses Netgear routers with modified firmware that enables the routers to phone home the broadband benchmark data collected. This rule would apparently invalidate the FCC's own survey project unless it hypocritically excludes these routers from the rule.

(I know about this modified firmware because I'm a project participant and have one of the modified routers.)

Isn't this delicious irony? The FCC's own "SamKnows" broadband survey project uses Netgear routers with modified firmware that enables the routers to phone home the broadband benchmark data collected. This rule would apparently invalidate the FCC's own survey project unless it hypocritically excludes these routers from the rule.

(I know about this modified firmware because I'm a project participant and have one of the modified routers.)

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: James

Last Name: McMahon

Mailing Address: 696 West Timothy Dr

City: La Porte

Country: United States

State or Province: IN

ZIP/Postal Code: 46350

Email Address:

Organization Name:

Comment: I wish to express my disagreement with this proposed FCC Regulation. I comprehend the desire to restrict malicious (unintentional or not) disruption to existing Wi-Fi networking by utilizing a base level DRM to prevent modifications of firmware code, however this proposed regulation goes too far. Allowing end users the opportunity to enhance the utility of their purchased physical devices through modifications in software are the essence of our modern computing platforms. I personally utilize DD-WRT on my home router as it allows me more flexibility in my system than the original firmware would ever do. I fear that implementation of this regulation would affect hundreds of thousands of end users like myself from being able to utilize a third party firmware to enhance and expand my ability to maintain and control my networking connections. Please revise this proposed regulation to expressly exempt the installation of third party firmware into electronic devices by the owners of those devices.

Sincerely Yours,

I wish to express my disagreement with this proposed FCC Regulation. I comprehend the desire to restrict malicious (unintentional or not) disruption to existing Wi-Fi networking by utilizing a base level DRM to prevent modifications of firmware code, however this proposed regulation goes too far. Allowing end users the opportunity to enhance the utility of their purchased physical devices through modifications in software are the essence of our modern computing platforms. I personally utilize DD-WRT on my home router as it allows me more flexibility in my system than the original firmware would ever do. I fear that implementation of this regulation would affect hundreds of thousands of end users like myself from being able to utilize a third party firmware to enhance and expand my ability to maintain and control my networking connections. Please revise this proposed regulation to expressly exempt the installation of third party firmware into electronic devices by the owners of those devices.

Sincerely Yours,

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Raymond

Last Name: Braun

Mailing Address: 109 Merle Cir

City: Fort Walton Beach

Country: United States

State or Province: FL

ZIP/Postal Code: 32547

Email Address: yew4439@gmail.com

Organization Name:

Comment: Perhaps you could be specific about what you wish to ban; indeed we can update our firmware and enable/modify features that will have no ill effects on the public wireless spectrum. I presume you are proposing this ban because of some concerns about interfering with other frequencies, etc?

Then ban that.

Dont ban hobbyists or enthusiasts from doing what we do.

Perhaps you could be specific about what you wish to ban; indeed we can update our firmware and enable/modify features that will have no ill effects on the public wireless spectrum. I presume you are proposing this ban because of some concerns about interfering with other frequencies, etc?

Then ban that.

Dont ban hobbyists or enthusiasts from doing what we do.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Michael

Last Name: Culver

Mailing Address: 565 woodlawn st

City: hoffman estates

Country: United States

State or Province: IL

ZIP/Postal Code: 60169

Email Address: mculver@gmail.com

Organization Name:

Comment: I don't think these rules are needed to prevent the rare occurrence of abuse. This would limit the use of plenty of really great open source firmware that give us end users tones of great functionality.

I don't think these rules are needed to prevent the rare occurrence of abuse. This would limit the use of plenty of really great open source firmware that give us end users tones of great functionality.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Garrett

Last Name: Burgwardt

Mailing Address: 5929 Broadway St

City: Lancaster

Country: United States

State or Province: NY

ZIP/Postal Code: 14086

Email Address:

Organization Name:

Comment: I buy the best router I can then put ddwrt on it (custom firmware) so that I get more options, better and more reliable QoS settings, etc. This proposed legislation seems to stop that, and is ridiculous. Please reconsider.

I buy the best router I can then put ddwrt on it (custom firmware) so that I get more options, better and more reliable QoS settings, etc. This proposed legislation seems to stop that, and is ridiculous. Please reconsider.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Tim

Last Name: Clark

Mailing Address: 10250 E Calle Magdalena

City: Tucson

Country: United States

State or Province: AZ

ZIP/Postal Code: 85748

Email Address: tim.clark.82@gmail.com

Organization Name:

Comment: Please do not do a blanket ban on all modified firmware. It makes more sense to ban misuse of the spectrum rules, but not a blanket ban on all modifications. OpenWRT and DD-WRT already obey regulatory rules and I don't see how banning them will help in any way.

Please do not do a blanket ban on all modified firmware. It makes more sense to ban misuse of the spectrum rules, but not a blanket ban on all modifications. OpenWRT and DD-WRT already obey regulatory rules and I don't see how banning them will help in any way.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jeffrey

Last Name: Melville

Mailing Address: 98 Central St Apt 1

City: Somerville

Country: United States

State or Province: MA

ZIP/Postal Code: 02143

Email Address: jeff.melville@gmail.com

Organization Name:

Comment: I would encourage the FCC not to adopt a requirement that would prevent me from loading new software on WiFi devices that I own. I have personally owned several WiFi routers that are plagued with unstable and/or insecure code. As a commodity item with a short product cycle, manufacturers simply do not have the resources or incentive to address all issues on their own. The community has filled this void by providing open source firmware that provides enhanced capabilities, security, and stability. Prohibiting further development and usage of these open source firmwares would be an unfortunate waste of effort and functionality.

I understand the concern to ensure that the massive number of commercial devices comply with the transmit limitations of the unlicensed bands they occupy. I also understand that the increasingly software-defined nature of these platforms makes it harder to ensure compliance at the hardware level. However, I strongly believe that the minimal increase in enforcement effort is justified to avoid stifling an innovative and beneficial usage path for these devices. To this point, I am not aware of an open source firmware that encourages or enables users to violate FCC regulations for unlicensed devices.

I appreciate your consideration in this matter.

I would encourage the FCC not to adopt a requirement that would prevent me from loading new software on WiFi devices that I own. I have personally owned several WiFi routers that are plagued with unstable and/or insecure code. As a commodity item with a short product cycle, manufacturers simply do not have the resources or incentive to address all issues on their own. The community has filled this void by providing open source firmware that provides enhanced capabilities, security, and stability. Prohibiting further development and usage of these open source firmwares would be an unfortunate waste of effort and functionality.

I understand the concern to ensure that the massive number of commercial devices comply with the transmit limitations of the unlicensed bands they occupy. I also understand that the increasingly software-defined nature of these platforms makes it harder to ensure compliance at the hardware level. However, I strongly believe that the minimal increase in enforcement effort is justified to avoid stifling an innovative and beneficial usage path for these devices. To this point, I am not aware of an open source firmware that encourages or enables users to violate FCC regulations for unlicensed devices.

I appreciate your consideration in this matter.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Joseph

Last Name: Trout

Mailing Address: 3601 silver brook st

City: Las Vegas

Country: United States

State or Province: NV

ZIP/Postal Code: 89129

Email Address: joseph@trouts.info

Organization Name:

Comment: FCC,

I was recently made aware of this proposed change specifically the issue that concerns me as a user is the effort to prevent modification of the firmware on devices that are capable of wireless transmission. I respect that some may have concerns regarding ability's that can be added to a router by something like openwrt or some other aftermarket firmware, as it may cause someone to buy a cheaper product and upgrade it themselves instead of buying a more expensive and still limited product. In my mind the only reason someone would limit firmware modification would be to line someones pocketbook.

There are benefits to allowing things to stay as they are though.

-Student and Researchers can actually afford devices, thus providing us with a better more experienced workforce, as well as better more efficient device designs

-These same Students and Researchers because of their expanded knowledge could also be able to fix security holes that have existed in the old firmware and provide help to the company that make these products thus saving company money and helping the population of the US more fully.

-Companies that live on making flexible hardware with update-able firmware may loose money. For instance: Instead of buying a TPLink router with modification which better fills your needs (Perhaps you combined your router and home server into one) Instead now you buy a cisco/linksys product that does not fill your needs but is more readily available Please do not implement "Equipment Authorization and Electronic Labeling for Wireless Devices"

Thank You

FCC,

I was recently made aware of this proposed change specifically the issue that concerns me as a user is the effort to prevent modification of the firmware on devices that are capable of wireless transmission. I respect that some may have concerns regarding ability's that can be added to a router by something like openwrt or some other aftermarket firmware, as it may cause someone to buy a cheaper product and upgrade it themselves instead of buying a more expensive and still limited product. In my mind the only reason someone would limit firmware modification would be to line someones pocketbook.

There are benefits to allowing things to stay as they are though.

-Student and Researchers can actually afford devices, thus providing us with a better more experienced workforce, as well as better more efficient device designs

-These same Students and Researchers because of their expanded knowledge could also be able to fix security holes that have existed in the old firmware and provide help to the company that make these products thus saving company money and helping the population of the US more fully.

-Companies that live on making flexible hardware with update-able firmware may loose money. For instance: Instead of

buying a TPLink router with modification which better fills your needs (Perhaps you combined your router and home server into one) Instead now you buy a cisco/linksys product that does not fill your needs but is more readily available Please do not implement "Equipment Authorization and Electronic Labeling for Wireless Devices"

Thank You

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Matthew

Last Name: Daugherty

Mailing Address: 8600 n FM 620 Apt 2437

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78726

Email Address: kf5rhg@arrl.net

Organization Name:

Comment: The devices need to be modifiable by third parties without needing to apply for certificates. Otherwise, invitation of the Open Source community will be discouraged, which will slow progress these devices as a whole.

This is also going to be detrimental to the meshnet used by amatuer radio operators in times of emergency. Degrading the meshnet will slow reaction time during emergency situations, which could put people's lives at stake.

This is also detrimental to internet security. Hardware manufacturers don't necessarily push security updates in a timely manner. The Open Source community allows for faster turnaround on bug patches and security updates.

The devices need to be modifiable by third parties without needing to apply for certificates. Otherwise, invitation of the Open Source community will be discouraged, which will slow progress these devices as a whole.

This is also going to be detrimental to the meshnet used by amatuer radio operators in times of emergency. Degrading the meshnet will slow reaction time during emergency situations, which could put people's lives at stake.

This is also detrimental to internet security. Hardware manufacturers don't necessarily push security updates in a timely manner. The Open Source community allows for faster turnaround on bug patches and security updates.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Garrett

Last Name: Calabrese

Mailing Address: 10 Octavia place

City: Keyport

Country: United States

State or Province: NJ

ZIP/Postal Code: 07735

Email Address:

Organization Name:

Comment: I strongly and respectfully urge the FCC not to implement these strict rules on the grounds that

1:(Wireless networking research depends on the ability of researchers to investigate and modify their devices)

Our country depends heavily on using wireless networking securely, and without the efforts of volunteer researchers being able to legally investigate and modify a device with security flaws, many devices and users will be left open to cyber criminals who care nothing for the law.

2:(Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.)

Lately We have been seeing a trend that a company will release a device such as a router or an ip camera and when there are security flaws found in the software, they refuse to fix the problem leaving many end user's privacy and personal information potentially vulnerable. Users in the past have been able to fix serious bugs in their wifi drivers, but that will be banned under the NPRM.

I strongly and respectfully urge the FCC not to implement these strict rules on the grounds that

1:(Wireless networking research depends on the ability of researchers to investigate and modify their devices)

Our country depends heavily on using wireless networking securely, and without the efforts of volunteer researchers being able to legally investigate and modify a device with security flaws, many devices and users will be left open to cyber criminals who care nothing for the law.

2:(Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.)

Lately We have been seeing a trend that a company will release a device such as a router or an ip camera and when there are security flaws found in the software, they refuse to fix the problem leaving many end user's privacy and personal information potentially vulnerable. Users in the past have been able to fix serious bugs in their wifi drivers, but that will be banned under the NPRM.



Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Donald

Last Name: Perdue

Mailing Address: 405 Foss Avenue

City: Belton

Country: United States

State or Province: MO

ZIP/Postal Code: 64012

Email Address: dperdue@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private

citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Peter

Last Name: Hiegel

Mailing Address: 398 William Ivey Rd SW

City: Lilburn

Country: United States

State or Province: GA

ZIP/Postal Code: 30047

Email Address: federalregister.gov@toyrobotworkshop.com

Organization Name:

Comment: The FCC is currently considering a proposal to lock down the firmware of electronic devices to prevent the modification of parameters that control the modular wireless radios on-board. Should this proposal go forward it would have significant and far reaching negative consequences beyond the intended purpose of preventing users from operating the radios outside of permissible configurations. One of the biggest problems facing the cellular industry today is that Carriers control the firmware installed on user handsets. When security issues arise, it's the Carrier's responsibility to update user handsets to fix those issues however this rarely occurs leaving users exposed to countless threats. The FCC proposal would force this problem on all electronic devices.

Currently there are countless open-source communities that generate custom firmwares for electronics that provide the latest and most secure software available for them. Often times, vendor firmware for devices are based of this work. If the FCC Proposal goes forward it would lock these communities out of supporting or maintaining these devices. It would also drive up the cost of electronic devices because vendors would need to rely on proprietary or commercial solutions that are currently free because the proposal would have destroyed the free option.

Please reconsider this proposal as it would have broad negative consequences on industry and put millions of Americans at risk from unknown security risks in the future.

The FCC is currently considering a proposal to lock down the firmware of electronic devices to prevent the modification of parameters that control the modular wireless radios on-board. Should this proposal go forward it would have significant and far reaching negative consequences beyond the intended purpose of preventing users from operating the radios outside of permissible configurations. One of the biggest problems facing the cellular industry today is that Carriers control the firmware installed on user handsets. When security issues arise, it's the Carrier's responsibility to update user handsets to fix those issues however this rarely occurs leaving users exposed to countless threats. The FCC proposal would force this problem on all electronic devices.

Currently there are countless open-source communities that generate custom firmwares for electronics that provide the latest and most secure software available for them. Often times, vendor firmware for devices are based of this work. If the FCC Proposal goes forward it would lock these communities out of supporting or maintaining these devices. It would also drive up the cost of electronic devices because vendors would need to rely on proprietary or commercial solutions that are currently free because the proposal would have destroyed the free option.

Please reconsider this proposal as it would have broad negative consequences on industry and put millions of Americans at risk from unknown security risks in the future.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Eric

Last Name: Hahn

Mailing Address: 845 Emerson Drive

City: Charlottesville

Country: United States

State or Province: VA

ZIP/Postal Code: 22901

Email Address: erichahn525@gmail.com

Organization Name:

Comment: Capitalism: an economic and political system in which a country's trade and industry are controlled by private owners for profit, rather than by the state.

By choosing to take away the ability of users to install the software of their choosing on their computing devices the FCC will partially remove capitalism from the public.

Secondly, wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would have be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I love the FCC, I love all the positive changes that have been made over the years, please do not take a step back in the wrong direction.

Capitalism: an economic and political system in which a country's trade and industry are controlled by private owners for profit, rather than by the state.

By choosing to take away the ability of users to install the software of their choosing on their computing devices the FCC will partially remove capitalism from the public.

Secondly, wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would have be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I love the FCC, I love all the positive changes that have been made over the years, please do not take a step back in the wrong direction.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Andrew

Last Name: Valencia

Mailing Address: PO Box 2221

City: Vashon

Country: United States

State or Province: WA

ZIP/Postal Code: 98070

Email Address: [ajv-itiaterestha@vsta.org](mailto:ajv-itiaterestha@vsta.org)

Organization Name: Voice of Vashon, Vashon Be Prepared

Comment: I am a Cisco Distinguished Engineer (retired) and a frequent volunteer in community networking projects--school district, local businesses, and emergency communications. Custom firmwares are a critical element of the way communities and smaller organizations (ones without the clout to get a large manufacturer to modify their device's firmware) can adopt innovative and cost effective networking solutions. They provide facilities in security, diagnostics, and custom user experiences which will probably never be addressed by "good enough for the average user" mentality of a large manufacturer.

Please do NOT drive these custom firmwares out of existence. They are a valuable source of solutions for communities.

I am a Cisco Distinguished Engineer (retired) and a frequent volunteer in community networking projects--school district, local businesses, and emergency communications. Custom firmwares are a critical element of the way communities and smaller organizations (ones without the clout to get a large manufacturer to modify their device's firmware) can adopt innovative and cost effective networking solutions. They provide facilities in security, diagnostics, and custom user experiences which will probably never be addressed by "good enough for the average user" mentality of a large manufacturer.

Please do NOT drive these custom firmwares out of existence. They are a valuable source of solutions for communities.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Khristopher

Last Name: Chireno

Mailing Address: 570 powell st

City: brooklyn

Country: United States

State or Province: NY

ZIP/Postal Code: 11212

Email Address: ksc154@gmail.com

Organization Name:

Comment: I would like to ask the FCC to not implement the proposal for Equipment Authrization and Electronic Labeling for Wireless Devices. I ask this because I have been directly affected by recieving faulty routers that would not be fixed by the seller to which I turned to open source router firmware. To allow a router I bought from being an expensive paper weight.

Not only did it allow me to use the router but also allowed me to learn and implement advanced security protocols to make sure my network and everyone on it is secure. Please don't implement this and stop the advancements that will ineveitably make the internet safer for everyone.

Thank you.

I would like to ask the FCC to not implement the proposal for Equipment Authrization and Electronic Labeling for Wireless Devices. I ask this because I have been directly affected by recieving faulty routers that would not be fixed by the seller to which I turned to open source router firmware. To allow a router I bought from being an expensive paper weight.

Not only did it allow me to use the router but also allowed me to learn and implement advanced security protocols to make sure my network and everyone on it is secure. Please don't implement this and stop the advancements that will ineveitably make the internet safer for everyone.

Thank you.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Frederic

Last Name: Roussel

Mailing Address: 3770 Flora Vista Ave APT 1701

City: Santa Clara

Country: United States

State or Province: CA

ZIP/Postal Code: 95051

Email Address:

Organization Name:

Comment: I am respectfully asking you to not implement rules that would prevent end users to install the software they have chosen on their computing equipment.

American people need to retain the ability to fix security holes in that equipment. At some point, manufacturers stop supporting the device they have sold. It is then up to the end user to keep their device safe in the face of quickly evolving threats.

A scenario to consider would be that my age old router is no longer supported by the vendor. It happens that a security hole exists in its firmware. At that point it would be open for grabs and could be used as a relay of sort by black hat hackers, be common scammer/spammer, international mafioso, spy from another unfriendly country, etc. It could also be made so open as to allow the aforementioned hackers to invade further into my home computers and thus gain access to valuable data.

If I lose the ability to monitor and fix the firmware, the old router could be used for illegal activity unbeknownst to me.

The same concerns would apply to all kind of equipment that would be restricted to be fixed and secured at the software/driver/firmware level.

Thank you for your consideration.

I am respectfully asking you to not implement rules that would prevent end users to install the software they have chosen on their computing equipment.

American people need to retain the ability to fix security holes in that equipment. At some point, manufacturers stop supporting the device they have sold. It is then up to the end user to keep their device safe in the face of quickly evolving threats.

A scenario to consider would be that my age old router is no longer supported by the vendor. It happens that a security hole exists in its firmware. At that point it would be open for grabs and could be used as a relay of sort by black hat hackers, be common scammer/spammer, international mafioso, spy from another unfriendly country, etc. It could also be made so open as to allow the aforementioned hackers to invade further into my home computers and

thus gain access to valuable data.

If I lose the ability to monitor and fix the firmware, the old router could be used for illegal activity unbeknownst to me.

The same concerns would apply to all kind of equipment that would be restricted to be fixed and secured at the software/driver/firmware level.

Thank you for your consideration.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Joseph

Last Name: Johnston

Mailing Address: 313 Foxglove Dr

City: Vicksburg

Country: United States

State or Province: TN

ZIP/Postal Code: 37211

Email Address: joseph.johnston@gmail.com

Organization Name:

Comment: Please reconsider this poorly thought-out proposition.

Please reconsider this poorly thought-out proposition.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Shawn

Last Name: Van Pelt

Mailing Address: 1325 Orange St.

City: Berwick

Country: United States

State or Province: PA

ZIP/Postal Code: 18603

Email Address:

Organization Name:

Comment: FCC please do not implement this new law. It can only cripple developement and application open source softwares and limit freedoms of users who purchase electronic devives.

FCC please do not implement this new law. It can only cripple developement and application open source softwares and limit freedoms of users who purchase electronic devives.